UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/785,722	02/16/2001	Hans Christopher Sowa	CM04812H	4254

22917 7590 01/19/2006

MOTOROLA, INC.
1303 EAST ALGONQUIN ROAD
IL01/3RD
SCHAUMBURG, IL 60196

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/785,722	SOWA ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48,52-71,73-91 and 93-98* is/are pending in the application.

4a) Of the above claim(s) *95-98* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *42-48,52-71,73-91,93 and 94* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/7/2005 has been entered.

During a telephone conversation with Attorney Valerie M. Davis on 01/10/2006, a provisional election was made without traverse to prosecute the invention of Group I: Claims 1 – 41. Affirmation of this election must be made by Applicant in replying to this Office action. Claims 42 – 48, 52 – 71, 73 – 91, 93 – 98 are withdrawn from further consideration by the Examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Election / Restrictions

This application contains claims directed to the following patentably distinct claimed inventions. Restriction to one of the following invention is required under 35 U.S.C 121:

I. (Group 1) Claims 1 – 41 drawn to an authentication method of securing air interface communications with a mobile station within a single zone, by using random number generation and the intra-key, classified in class 380, subclass 262.

II. (Group 2) Claims 42 – 48, 52 – 71, 73 – 91, 93 and 94 drawn to a method of securing air interface communications for mobile stations with position-dependent authentications covering at least more than two zones using not only the intra-key but also the inter-key, classified in class 380, subclass 258.

III. (Group 3) Claims 95 – 98 drawn to a more specific mobile station power-down/up management, classified in class 380, subclass 249.

Inventions I – III are related as subcombination disclosed as usable together in a single combination. The subcombination is distinct from the combination and the subcombinations are distinct from each other if they are shown to be separately usable. The following case instants:

Invention I has utility directed to an authentication method of securing air interface communications with a mobile station within a single zone, by using random number and random seed generation as well as the intra-key which is used for encrypting key material distributed within the first / same zone.

Invention II has separate utility directed to a method of securing air interface communications for mobile stations with position-dependent authentications that covers at least more than two zones using not only the intra-key but also the inter-key used for encrypting the first zone authentication information for transport to another system device in a zone other than the first zone.

Invention III has separate utility directed to mobile station with the features more specific to its power-down/up management.

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification and utility restriction for examination purpose as indicated is proper.

Examiner acknowledges that Applicant has elected Group I and as such this Office action only addresses the claimed inventions of Group I: Claims 1 – 41.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1 – 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Terrestrial Trunked Radio (TETRA) Voice Plus Data (V+D) Part 7: Security" (EN 300 392-7 V2.0.19, 2000-11), hereinafter referred to as TETRA-2000, in view of Roelofsen ("TETRA Security").

As per claim 1 and 23, TETRA-2000 teaches a method comprising the steps of:

generating a random number, an expected response, and a derived cipher key associated with securing air interface communications with a mobile station (TETRA-2000: Figure 1 and Section 4.1.2);

forwarding the random number and a random seed to a base station that is located in a first pool of devices (TETRA-2000: Section 4.1.1 Line 6 – 7), wherein the first pool is associated with an intrakey used for encrypting key material that is distributed within the first pool (TETRA-2000: Section 6.5.1.3, Section 4.2.2 and Section 4.2.4 (Page 25 / 4th Para): the intrakey is equivalent to either of Common Cipger Key (CCK), Group Cipher Key (GCK) or Static Cipher Key (SCK) when either one of them is used to be associated with a particular group / location area);

receiving, from the base station, a response to the random number and the random seed (TETRA-2000: Figure 3);

comparing the response and the expected response (TETRA-2000: Section 4.1.2); and

TETRA-2000 teaches when the response matches the expected response, forwarding the derived cipher key to the base station (TETRA-2000: Section 4.2.1 / the

last paragraph and Section 6.6.2.4 / 3rd Para). However, TETRA-2000 does not disclose expressly encrypting the derived cipher key using the intrakey and forwarding the encrypted derived cipher key to the base station.

Roelofsen teaches encrypting the derived cipher key using the intrakey and forwarding the encrypted derived cipher key to the base station (Roelofsen: Page 50 / the last Para and Page 51 / 3rd Para / Line 13 – 15 & TETRA-2000: Section 4.2.3 Line 8: the key may be derived and transferred as part of the authentication procedure).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Roelofsen within the system of TETRA-2000 because (a) TETRA-2000 discloses key-encrypting-key (KEK) can enhance the security on transferring the sensitive information, especially both of derived cipher key and CCK / GCK / SCK (intrakey) are independently generated (TETRA-2000: Section 4.2.3 Line 8), and (b) Roelofsen teaches the key may be derived and transferred as part of the authentication procedure and SCK can be used for encryption in situations where authentication has not yet been completed and as such derived cipher key (DCK) is not yet available to be used (Roelofsen: Page 50 / the last Para and Page 51 / 3rd Para / Line 13 – 15).

As per claim 16 and 36, TETRA-2000 teaches a method performed by any of a base station and comprising the steps of:

receiving an authentication request from a mobile station; determining whether to forward the request to an authentication agent; and when it is determined to forward the

request, forwarding the request to the authentication agent (TETRA-2000: Section 4.1.1 Line 8 – 10 & Figure 1 and Section 4.1.2: The base station may carry out the authentication protocols between the mobile station and authentication agent);

receiving a random number and a random seed from the authentication agent; and forwarding the random number and the random seed to the mobile station (TETRA-2000: Figure 1);

receiving a response to the random number and the random seed from the mobile station and forwarding the response to the authentication agent (TETRA-2000: Figure 1);

TETRA-2000 teaches when the authentication agent authenticates the mobile station, receiving from the authentication agent the derived cipher key and forwarding to the mobile station (TETRA-2000: Section 4.2.1 / the and Section 6.6.2.4 / 3rd Para paragraph) and using an intrakey for the first pool (TETRA-2000: Section 6.5.1.3, Section 4.2.2 and Section 4.2.4 (Page 25 / 4th Para): the intrakey is equivalent to either of Common Cipger Key (CCK), Group Cipher Key (GCK) or Static Cipher Key (SCK) when either one of them is used to be associated with a particular group / location area). However, TETRA-2000 does not disclose expressly using the intrakey to encrypt the derived cipher key when forwarding the key material to the mobile station.

Roelofsen teaches encrypting the derived cipher key using the intrakey and forwarding the encrypted derived cipher key to the mobile station (Roelofsen: Page 50 / the last Para and Page 51 / 3rd Para / Line 13 – 15 & TETRA-2000: Section 4.2.3 Line 8: the key may be derived and transferred as part of the authentication procedure).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Roelofsen within the system of TETRA-2000 because (a) TETRA-2000 discloses key-encrypting-key (KEK) can enhance the security on transferring the sensitive information, especially both of derived cipher key and CCK / GCK / SCK (intrakey) are independently generated (TETRA-2000: Section 4.2.3 Line 8), and (b) Roelofsen teaches the key may be derived and transferred as part of the authentication procedure and SCK can be used for encryption in situations where authentication has not yet been completed and as such derived cipher key (DCK) is not yet available to be used (Roelofsen: Page 50 / the last Para and Page 51 / 3rd Para / Line 13 – 15).

encrypting messages to the mobile station and decrypting messages from the mobile station with the derived cipher key. (TETRA-2000: TETRA-2000: Section 4.2.1 / the last paragraph and Section 6.6.2.4 / 3rd Para).

As per claims 2, 24 and 37, TETRA-2000 teaches when the response does not match the expected response, discarding the derived cipher key without encrypting the derived cipher key and forwarding the encrypted derived cipher key to the base station (TETRA-2000: Section 4.1.2 Line 9 – 10).

As per claims 3 and 17, TETRA-2000 as modified teaches sending a failed authentication message to the base station (TETRA-2000: Section 4.1.2 Line 9 – 10 and Figure 1).

As per claims 4 and 25, TETRA-2000 as modified teaches the expected response is generated at least indirectly from the random number and the random seed (TETRA-2000: see for example, Section 4.1.2 and Figure 1).

As per claims 5 and 26, TETRA-2000 as modified the derived cipher key is generated at least indirectly from the random number and the random seed (TETRA-2000: see for example, Section 4.1.2 and Figure 1).

As per claims 6, 8, 27 and 29, TETRA-2000 as modified teaches the derived cipher key (DCK) is stored at a visited location register (TETRA-2000: see for example, Section 4.1.5 Line 2 – 3 & Roelofsen: Page 52 Line 14 – 20: the mobile station always need to be identified (such as by the well-known visited center (e.g. well-known VLR / HLR) before the ciphering key is available and valid for use to help prevent user fraud and thereby the cipher key must be stored at the visited center such as VLR / HLR).

As per claims 7, 9, 28 and 30, TETRA-2000 as modified teaches the derived cipher key (DCK) is encrypted using the intrakey before being stored at the visited location register (Roelofsen: Page 50 / the last Para and Page 51 / 3rd Para / Line 13 – 15, Page 51 / the last Para & TETRA-2000: Section 4.2.3 Line 8: the key may be derived and transferred (stored) as part of the authentication procedure).

As per claims 10, 11, 18, 19, 31, 32, 38 and 39, TETRA-2000 as modified teaches the steps are performed by a zone controller (TETRA-2000: see for example, Section 4.1.1 Line 6 – 7 and Figure 1 & Roelofsen: Page 51 / the last Para: TETRA-2000 teaches the protocol exchange is between the authentication center and mobile station. Therefore, it is evident that the well-known HLR/VLR (or zone controller) and base station should all be involved to carry out this authentication protocols).

As per claim 12, TETRA-2000 as modified teaches the response is generated by a mobile station (TETRA-2000: see for example, Figure 1: RES1 (Response 1) is sent from MS to AuC in Figure 1).

As per claim 13, 20, 33 and 40, TETRA-2000 as modified teaches wherein the first pool comprises a first zone (TETRA-2000: Section 4.1.1 Line 6 – 7), wherein the first pool is associated with an intrakey used for encrypting key material that is distributed within the first pool (TETRA-2000: Section 6.5.1.3, Section 4.2.2 and Section 4.2.4 (Page 25 / 4th Para): the intrakey is equivalent to either of Common Cipger Key (CCK), Group Cipher Key (GCK) or Static Cipher Key (SCK) when either one of them is used to be associated with a particular group / location area).

As per claims 14, 21, 34 and 41, TETRA-2000 as modified teaches any of a base site and a TETRA site controller takes the place of the base station (TETRA-2000: see for example, Section 4.1.1 Line 6 – 7 and Figure 1 and Roelofsen: Page 51 / the last

Para: TETRA-2000 teaches the protocol exchange is between the authentication center and mobile station. Therefore, it is evident that HLR/VLR (or zone controller) and base station controller should all be involved to carry out this authentication protocols).

As per claim 15 and 22, TETRA-2000 as modified teaches receiving, from the base station, a second random number generated by a mobile station (TETRA-2000: see for example, Figure 6 & Figure 4 and Section 4.2.1 and Section 4.1.1 / 2nd Para);

generating a second derived cipher key and a second response to the second random number and forwarding the second response to the base station, the second derived cipher key also associated with securing the air interface communication with the mobile station (TETRA-2000: see for example, Figure 6 & Figure 4 and Section 4.2.1 and Section 4.1.1 / 2nd Para);

combining the derived cipher key and the second derived cipher key, yielding a third derived cipher key used for encrypting the air interface communication with the mobile station (TETRA-2000: see for example, Figure 6 & Figure 4);

when a positive authentication message is received from the base station, encrypting the third derived cipher key using the intrakey and forwarding the third derived cipher key to the base station (TETRA-2000: see for example, Section 4.2.1 and Figure 6 & 4 // Roelofsen: Page 50 / the last Para and Page 51 / 3rd Para / Line 13 – 15 & TETRA-2000: Section 4.2.3 Line 8: the key may be derived and transferred as part of the authentication procedure).

As per claim 35, TETRA-2000 as modified teaches the method is of a mutual authentication process (TETRA-2000: see for example, Section 4.1.4).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LBC

Longbit Chai
Examiner
Art Unit 2131

Primary Examiner
AU 2131
1/13/06